UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,874	12/14/2001	Jonathan Edwards	19903.0011	1766

23517 7590 05/04/2005

SWIDLER BERLIN LLP
3000 K STREET, NW
BOX IP
WASHINGTON, DC 20007

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/014,874	EDWARDS ET AL.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 December 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/02 & 12/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on December 11, 2003. No preliminary amendments to the specification were filed. Claims 1 – 36 are pending.

Information Disclosure Statement

2. Two initialed and dated copies of Applicant's IDS form 1449 are attached to the Office action.

Drawings

3. The drawings are objected to because in Fig. 4, steps 410 – 416 form an infinite loop. Examiner suggests step 420 to continue Process Execution and/or Finish process execution.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for

consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Detecting Malwares by Scanning a loaded process.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 – 36 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Drake (6,006,328).

6. As per Claim 1, Drake teaches

interrupting execution of a process that has been loaded for execution (Column 6 lines 6 – 20 and Column 7 lines 21 – 35 and 53 – 65);

scanning the process for a malware (Column 6 lines 6 – 20; Column 7 lines 21 – 35 and 53 – 65 and Column 17 line 1 – Column 18 line 43);

allowing the process to execute, if no malware is found (Column 18 lines 26 – 43); and

terminating execution of the process, if a malware is found (Column 6 lines 33 – 43).

7. As per Claim 13, Drake teaches

a processor operable to execute computer program instructions (Column 9 lines 50 – 57);

a memory operable to store computer program instructions executable by the processor (Column 9 lines 50 – 57); and

computer program instructions stored in the memory and executable to perform the steps of:

interrupting execution of a process that has been loaded for execution (Column 6 lines 6 – 20 and Column 7 lines 21 – 35 and 53 – 65);

scanning the process for a malware (Column 6 lines 6 – 20; Column 7 lines 21 – 35 and 53 – 65 and Column 17 line 1 – Column 18 line 43);

allowing the process to execute, if no malware is found (Column 18 lines 26 – 43); and

terminating execution of the process, if a malware is found (Column 6 lines 33 – 43).

8. As per Claim 25, Drake teaches

a computer readable medium (Column 8 lines 24 – 30);

computer program instructions, recorded on the computer readable medium, executable by a processor, for performing the steps of

interrupting execution of a process that has been loaded for execution (Column 6 lines 6 – 20 and Column 7 lines 21 – 35 and 53 – 65);

scanning the process for a malware (Column 6 lines 6 – 20; Column 7 lines 21 – 35 and 53 – 65 and Column 17 line 1 – Column 18 line 43);

allowing the process to execute, if no malware is found (Column 18 lines 26 – 43); and

terminating execution of the process, if a malware is found (Column 6 lines 33 – 43).

9. As per Claims 2, 14 and 26, Drake further teaches wherein the process is associated with an application program (Column 9 lines 50 – 57).

10. As per Claims 3, 15 and 27, Drake further teaches wherein the process is loaded from at least one compressed, packed, or encrypted file (Column 4 lines 48 – 65 and Column 14 lines 7 – 32).

11. As per Claims 4, 16 and 28, Drake further teaches loading code for execution by the process from at least one compressed, packed, or encrypted file (Column 4 lines 48 – 65; Column 6 lines 6 – 20 and Column 14 lines 7 – 32).

12. As per Claims 5, 17 and 29, Drake further teaches interrupting execution of the process when the process accesses at least one file that is not needed to perform decryption, decompression, or unpacking (Column 6 lines 6 – 32).

13. As per Claims 6, 18 and 30, Drake further teaches wherein the at least one tile that is not needed to perform decryption, decompression, or unpacking comprises a system library file (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

14. As per Claims 7, 19 and 31, Drake further teaches wherein the at least one file that is not needed to perform decryption, decompression, or unpacking comprises an executable file not related to the process (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

15. As per Claims 8, 20 and 32, Drake further teaches wherein the at least one file that is not needed to perform decryption, decompression, or unpacking comprises a data file not related to the process (Column 4 lines 47 – 65 and Column 6 lines 6 – 32).

16. As per Claims 9, 21 and 33, Drake further teaches wherein the malware is a computer virus (Column 1 line 56 – Column 2 line 62).

17. As per Claims 10, 22 and 34, Drake further teaches wherein the malware is a computer worm (Column 1 line 56 – Column 2 line 62).

18. As per Claims 11, 23 and 35, Drake further teaches wherein the malware is a Trojan horse program (Column 1 line 56 – Column 2 line 62).

19. As per Claims 12, 24 and 36, Drake further teaches scanning the process for a malware before execution of the process (Column 1 line 56 – Column 2 line 62 and Column 3 lines 33 – 67).

Conclusion

20. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are

applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. The prior art submitted by applicant has been considered by the examiner and made of record in the file. If applicants are aware of any better prior ad than those are cited, they are required to bring the prior art to the attention of the examiner.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
April 29, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100